USAWC STRATEGY RESEARCH PROJECT

THE DARK FRUIT OF GLOBALIZATION: HOSTILE USE OF THE INTERNET

by

Lieutenant Colonel Todd A. Megill
United States Army

Colonel David Brooks
Project Adviser

U.S. Army War College
CARLISLE BARRACKS, PENNSYLVANIA 17013

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
18 MAR 2005		-

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
The Dark Fruit of Globalization Hostile Use of the Internet	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
Todd Megill	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)	8. PERFORMING ORGANIZATION REPORT NUMBER
U.S. Army War College,Carlisle Barracks,Carlisle,PA,17013-5050	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT
See attached.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**		**22**	

ABSTRACT

AUTHOR: Lieutenant Colonel Todd A. Megill

TITLE: The Dark Fruit Of Globalization: Hostile Use Of The Internet

FORMAT: Strategy Research Project

DATE: 18 March 2005 PAGES: 22 CLASSIFICATION: Unclassified

One of the goals of the current National Security Strategy is to expand world economic activity and prosperity. This goal for economic prosperity is linked to globalization and this information technologies that tie the world's economics and occupants together. A primary means of communication and information sharing is the Internet. The United States (US) is currently the world's largest user and proponent of the Internet. The massive sharing of information is crucial for US economic development and expansion and is in line with the American concept of itself. However, the Internet, as a method of sharing information has a dark side. The information accessible, level of communications, linkages, and sheer interconnectiveness of the World-Wide-Web leaves the US vulnerable to violent non-state actors using the Internet. These groups will use the Internet and its architecture to command & control, collect information, target, possibly attack, access, and disseminate the results of their activities with minimal exposure to traditional means of national intelligence collection and detection. The architecture is allowing violent non-state actors to attack the US over its own systems and designs. This paper will look at this phenomenon, the scope of the problem, draw conclusions, and make some recommendations.

TABLE OF CONTENTS

THE DARK FRUIT OF GLOBALIZATION: HOSTILE USE OF THE INTERNET

One of the second order effects of an internet connected world, a direct consequence of increasing economic globalization and technological diffusion, is that insurgent/terrorist organizations who are most against the process of globalization are using its infrastructure to target and attack its biggest proponent, the US. The US, as the world's greatest power and leading engine of change, has created through the internet a "virtual global commons," and is increasingly used by anti-American and anti-globalization groups to conduct propaganda and plan attacks. This paper will focus on the internet, developed as an agent of economic change, being used by insurgents/terrorists to operate and conduct targeting operations employing a similar methodology adopted by the US Department of Defense.

US NATIONAL SECURITY, ECONOMIC PROSPERITY AND THE INTERNET

One of the major goals of the current US National Security Strategy[1] is to create and expand the world economy as a means for addressing some of the underlying causes of violence around the globe:

> A Strong World Economy enhances our national security by advancing prosperity and freedom in the rest of the world. Economic growth supported by free trade and free markets creates new jobs and higher incomes. It allows people to lift their lives out of poverty, spurs economic and legal reform, and the fight against corruption, and it reinforces the habits of liberty.[2]

Creating a strong world economy will lead the US even more toward embracing the concept and trends of Globalization: "Globalization refers to those entrenched and enduring patterns of worldwide interconnectiveness…it suggests that a growing magnitude or intensity of global flows such as that the states and societies become increasingly enmeshed in worldwide systems and networks of interaction."[3] The process of globalization, though initially created by US technical creativity and economic power, is now truly a global phenomenon as millions around the world contribute their expertise, creativity, and economic capital.

> Globalization isn't a choice. It's a reality. There is just one global market today, and the only way you can grow at the speed your people want is by tapping into the global stock and bond markets, by seeking out multinationals to invest in your country and by selling into the global trading system what your factories produce. And the most basic truth about globalization is this: No one is in charge- not George Soros, not 'Great Powers' and not I.[4]

Technological advances in telecommunications and computerization leading to the creation of the internet are the leading characteristics of the process involved in globalization.

"Today's era of globalization is built around falling telecommunication costs – thanks to microchips, satellites, fiber optics and the internet."[5]

If the global movement of goods and services are the lifeblood of the world economy then the internet is the nervous system, passing, collecting, and storing information that guides and directs such flows. The movement of information and data across the internet is so vast and pervasive in the US and the industrialized world in particular that it has become a feature of modern life. Air travel, sea travel, land travel, and now virtual travel that cross these global commons are the norm. A commons represents a shared resource or area with poorly defined boundaries, widely used or accessible, with limited supervision or governance. The last form of travel has no association with geography, possesses no boundaries, and is limited only by access to the World Wide Web. The internet is a continually expanding virtual commons of information and communication stretching across the globe.

THE IMPACT OF A VIRTUAL GLOBAL COMMONS

The major impact of the internet is that it has evolved into the fourth global commons. There is a terrestrial commons of land masses, an oceanic global commons that encompasses most of the globe, and an aerospace global commons that covers the earth and extends upward until you run out of atmosphere.[6] The internet has created a virtual global commons that extends as far as communications can reach and man has a desire to create an interface.

The virtual global commons that the internet provides for hostile users is unique and expands the opportunities for insurgency, criminality, terrorism, or other violent acts across the globe. There is little common agreement on the terms of terrorism or insurgency or if the current wave of Muslim fundamentalist extremism is political movement linked to an insurgency or random terrorist acts.[7] The use of the internet for violence does not predispose any political goal or objective and so the term terrorist/insurgent is used in this discussion. The worldwide internet allows the hostile terrorist/insurgent to create and/or occupy a "Distributed Sanctuary." The US Joint Chiefs of Staff defines a sanctuary as: "A nation or area near or contiguous to the combat area which by tacit agreement between the warring powers is exempt from attack and therefore serves as a refuge for staging, logistic, or other activities of the combatant powers."[8] The worldwide internet allows an expansion of that definition. The refuge or sanctuary no longer has to be near or contiguous to the area of combat or operations. The linkages provided by the worldwide internet allow the insurgent/terrorist to remain removed from the location he plans to attack. "The knowledge of how to conduct an attack is developed in one country, then that knowledge is combined with the raw materials, personnel, and training available in other

countries, which can include the target country, to create a weapon in the target country." [9] Options now exist to divide a sanctuary further, not only by location but by function. The world-wide internet allows an organization's fund raising to occur around the globe and its collection to be handled in a country that looks favorably upon the terrorist/insurgent's goals. "Al Qaeda appears to have relied on a core group of financial facilitators who raised money from a variety of donors and other fund-raisers, primarily in the Gulf countries and particularly in Saudi Arabia. "[10] Terrorist/insurgents use existing legal and illegal networks to gain financing including the use of free trade zones and the informal hawala system of currency transfers, including diamonds and gold.[11] The monies sent to terrorists/insurgents, planning operations in another location or in a nation-state, to locations with weak banking and financial laws allows them to launder the monies collected.

> Money laundering involves disguising assets so they can be used without detection of the illegal activity that produced them…This process has devastating social consequences. For one thing, money laundering provides the fuel for drug dealers, terrorists, arms dealers, and other criminals to operate and expand their operations[12].

The insurgent/terrorist can reside in a country where they are breaking no public laws and maintain a low profile. In a second country or location, other members procure and assemble the weapons or explosives for shipment to marry up with the actual attackers in yet a third country or location. The terrorist/insurgent attackers can flee or return to possibly a fourth country, the operation monitored by the group's leadership using news outlets and media access from yet another country. Finally, the terrorist/insurgents would develop the group's message and disseminate it throughout the world via the worldwide internet. Separating the various functions of insurgent/terrorist sustainment and operations or the phases of the targeting and attack methodology makes it difficult for national police of public security organizations to track and or gather evidence of criminal misconduct. "The old police technique of tracking illegal activity by watching certain places and peoples does not work when communications is carried out on line."[13]

> As we now know, support networks in Muslim diasporas, especially in Europe have been key nodes in the funding and operations of extremist and terrorist groups. Ironically, the activities of these groups have been facilitated by the reluctance of Western security and law enforcement agencies to monitor the activities of allegedly religious groups. As in the investigations following the events of September 11, 2001 have run their course, it has become apparent that Muslim diasporas in countries such as Germany, the United kingdom, France, Spain, Belgium, and Switzerland have been implicated as important hubs of Al Qaeda operations and recruitment.[14]

One of the challenges that the worldwide internet poses as a virtual global commons is that it already exists as an exploitable environment for criminals and insurgent/terrorists. It has the ability to be present or embedded into every aspect of mankind's existence. Thus, insurgent/terrorists do not have to expend much time, effort and money to painfully build the infrastructure for attack or revolt. The painstaking process of building cells, organizations and networks and the risks of communicating with them greatly decrease when done remotely. "Even more challenging from a security point of view is that the people do not have to go out to establish these networks. They do not have to be in the same country or even on line at the same time. "[15]

The internet is such a useful communications and economic tool that it is unlikely that a modern society can operate without it. The world economy, linked through a global communications network, has helped to raise the standard of living of millions around the world[16]. However, this communications infrastructure also brings change to much of the world. For those that do not want change and seek to deny it the internet can become a tool for attack and violent opposition to the very bodies, values, and organizations that helped to create it.[17] The Internet allows for a criminal, an insurgent, or a terrorist to expand his or her area of operations and gather the necessary information about targets they wish to exploit or attack without a physical presence until the actual tactical operation or attack occurs.

DOCTRINE: OURS AND THEIRS

In the US Military, at the Joint level, the doctrinal underpinnings of the targeting process are promulgated in Joint Pub 3-60, Joint Doctrine for Targeting, dated 17 January 2002.[18] The six-step process is used to define targets for attack in support of combat operations. The six-steps are as follows: 1-Commander's Objectives, Guidance and Intent, 2-Target Development, Validation, Nomination, and Prioritization, 3-Capabilities Analysis, 4-Commander's Decision and Force Assignment, 5-Mission Planning and Force Execution, and 6- Combat Assessment. Within this process, the US Army and US Marine Corps use the Decide, Detect, Deliver, and Assess Cycle (D3A) to support planning and link with the Joint Targeting Cycle.[19]

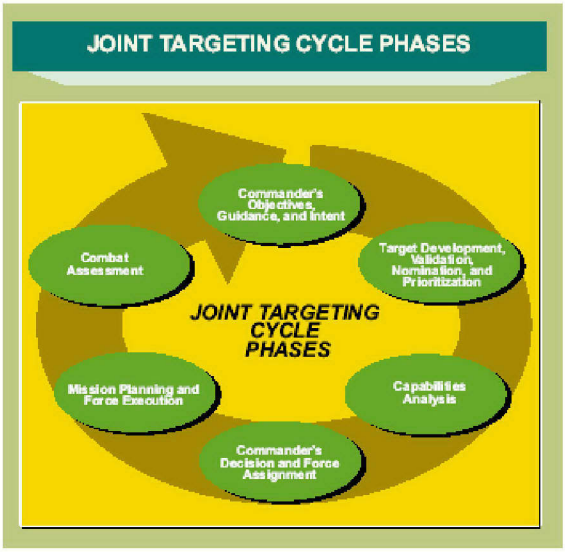

FIGURE 1. THE JOINT TARGETING CYCLE

This methodology is similar in many ways to the type of process that insurgents or terrorists use in defining, developing, and executing their attacks.[20] Moreover, the interconnectiveness of modern society and the presence of the internet allow the insurgents/terrorists to accomplish many of these steps from a distributed sanctuary, removed from the actual geographic location or population they intend to attack.

COMMANDER'S OBJECTIVES, GUIDANCE, AND INTENT

In both the US Military and an insurgent/terrorist organization, there are policy objectives achieved by the application of force or the threat of force. Both organizations provide this guidance and intent to subordinates in different forms: written documents, oral presentations, conversations, and graphics, stories, and pictures.[21] The internet makes this important step easier, as it allows those physically separated to maintain a high level of contact and communication.

> There used to be trade-off, they argue, between the reach of a message and its richness. A rich, detailed message required a one-on-one conversation; reaching out to thousands, for example, through advertising, meant you could send only simplistic messages. The tradeoff has now been killed by the new technologies: you can have rich, detailed customized information flowing from one to thousands or millions.[22]

The internet allows the communication of a leader's or commander's intent and guidance to his or her subordinates accurately, without the risk of actual physical contact that could lead to identification, arrest, or attack.

TARGET DEVELOPMENT, VALIDATION, NOMINATION, AND PRIORITIZATION AND CAPABILITIES ANALYSIS

This is the step that involves target selection. The US Army's decide phase in the D3A Cycle is embedded in this as military personnel decide what on the type of targets, where they are, who can locate them, and how they should be attacked.[23] This is a give-and-take process between intelligence and operations functions. A process that debates, assembles, and selects targets for lethal or non-lethal attack. Additionally, the evaluation and selection of the target results in the identification of the type of attack system or methodology likely employed against the nominated target. Again, the internet allows the insurgent/terrorist a similar capacity to communicate accurately over vast distances and keep track of individuals, ideas, and targets. The internet is an interconnected assemblage of databases that provides the insurgents/terrorists a low-cost, low-risk way of gathering information about their enemies. The Al Qaeda organization, a recent example of an evolving insurgent/terrorist network, uses computers and the internet as a matter of course to operate their organization and identify targets.

> Al Qaeda was a modern army. It was as adept with computers as any organization founded by the engineer son of a construction millionaire and staffed by largely by middle-class educated males. Intercepting Al Qaeda communications was hard mainly because the organization understood information technology so well.[24]

Expertise with information technology and the internet allows the insurgents/terrorists to gather the information needed to conduct their planning, targeting, and weaponeering remotely:

> Meanwhile, Al Qaeda operatives used the Internet to scope out targets. They downloaded layouts of bridges and buildings from Web sites. In the past, collecting this kind of information might require traveling around the world. Getting it to someone in the field required undercover couriers. Now you could click, get the data, click again, and send the diagrams to a temporary, untraceable e-mail address.[25]

A translation of an Al Qaeda Training manual gives clear guidance to followers and operatives on how to gather information/intelligence about an enemy or target:

> Any organization that desires to raise the flag of Islam high and proud must gather as much information as possible about the enemy. Information has two sources:

> Public Sources: Using public sources openly and without resorting to illegal means, it is possible to gather at least 80 percent of the information available about the enemy…The one gathering the information should be a regular person (trained college graduate) who examines primary sources of information published by the enemy (newspapers, magazines, radio, TV, etc.)…The one gathering information with this public method is not exposed to any danger whatsoever. Any brother can gather information from those aforementioned sources.[26]

The internet makes it possible for a global insurgency or terrorist networked organization to exist. Prior to the invention and dissemination of the internet, geography had a great influence on the movement of information. The physical distance between members made communications and information collection much slower, riskier, and time consuming.

COMMANDER'S DECISION AND FORCE ASSIGNMENT AND MISSION PLANNING AND FORCE EXECUTION

These two phases are so closely intertwined that they can occur near simultaneously. Now the commander approves selected targets, which are then attacked. In US Army doctrine, this is the deliver phase of the D3A Cycle. The US military and the insurgents/terrorist have a number of ways of attacking the target(s) and the US military has the advantage in possessing specialized weapons that can afford it considerable target standoff and destructive power. The insurgent/terrorist currently has neither the standoff nor destructive capability of the US military, but it has its own enormous capability.

> The advance of technology is why we now worry about weapons of mass destruction. For the first time in history, a single attacker may be able to use technology to kill millions of people…Technology will continue to alter the balance between the attacker and the defender, at an ever-increasing pace. In addition, technology will generally favor the attacker, with the defender playing catch-up.[27]

The President of the US has stated in the National Security Strategy "The gravest danger our Nation faces lies at the crossroads of radicalism and technology."[28]

The internet can serve as a command, control, communications, computerization, and intelligence to facilitate lethal attacks. In addition, there is a growing body of literature that indicates it could be the actual attack mechanism to disable or disrupt certain components of a modern industrialized society.[29] Again, the insurgent/terrorist need not be physically present in relation to the target when conducting such an attack.

COMBAT ASSESSMENT

The Joint Targeting Process's final phase, mirrored in the US Army D3A Cycle, is the assessment phase. This is the estimate of the damage resulting from the use of force.[30] The US military uses intelligence and operational assets to evaluate the damage to the target and assess if the commander's desired level of effect is achieved. It the needed level of effect is not achieved then the target is prioritized for another attack. The insurgent/terrorist organization evaluates a successfully attacked target in relation to its symbolic and propaganda value. The internet greatly facilitates this evaluation as it grants nearly real-time knowledge of the attack and target impact due to the world media presence. An insurgent/terrorist attack is big news in most of the world and the near immediate broadcasts of images of the attack help the terrorist/insurgent evaluate his success. In a crude way, the sheer amount of reporting on a given attack can give the insurgent/terrorist an idea of how successful the organization's attack was. Monitoring multiple media outlets from around the world is easy to do on the internet. The internet allows the insurgents/terrorists to monitor their attack at the same time they advertise their activities and promote their views and cause. This then completes the targeting process with the organization's message being enhanced or modified. The targeting process begins again with the insurgent/terrorist looking for new targets to attack. The internet allows this targeting process to occur across the globe with the insurgent/terrorist network being connected by the thinnest web of electrons via the internet.

CONCLUSION

The expanding use of the internet lies at the heart of the globalizing world economy. The interconnectiveness of the financial and business sectors around the world is critical to the quality of life and standard of living of Americans. The US, in an effort to improve its national security posture, actively promotes the global economy as a way to address numerous social evils and promote basic human rights.[31] The internet is a means of more firmly integrating all the nations and peoples of the world into more interconnected and stable political units. This allows increased efficiencies that translate into economic improvements. However, the internet brings both opportunities and threats. It is a method of improving efficiencies and linkages between people and businesses. It also serves as a tool for those opposed to the globalized political economy to tap into the fears of dynamic change and carry-on a networked anti-American insurgency.

The targeting methodology that the US military uses at the joint level is similar at both the operational/strategic and tactical levels to how global insurgents/terrorists can now conduct their

own operations using the internet. The ability to send clear, concise, information dense messages across the world enhances the insurgent's security, no longer having to meet face-to-face to encourage members and plan. The internet allows individuals and small groups with common agendas to easily make and maintain contact with each other. The internet serves as a global venue to disseminate their message or vision. The internet not only provides a highly effective means of organizing, commanding, and controlling an insurgency/terrorist network, but also serves as a highly useful tool to collect targeting information for future attacks. Terrorist/insurgents can conduct operational planning, target evaluation, initial weaponeering, and a post-attack assessment without physically visiting the intended target. This remote targeting process, buried in the mass of traffic and data that flows across the World Wide Web makes it very difficult for security forces to track insurgent/terrorist activities. The internet allows the insurgents/terrorists to expose themselves to a minimal amount of risk of capture until the actual execution of the targeted attack. After attacking the target, the organization can monitor its success nearly instantaneously at almost no cost or risk to itself. Finally, the internet allows the insurgents/terrorist to trumpet their activities when they chose to do so throughout the world, again both quickly and with relative security.

The internet allows the establishment of a worldwide insurgency by non-state actors. Super empowered angry young men can link themselves together via the internet and become a cohesive organization networked together.[32] The insurgents/terrorists seldom need to come together to remain a functional organization. The internet allows insurgent/terrorists to be scattered across the globe and hidden in small groups, They need not come together to operate creating a very difficult signature for security officials to find. The internet is a growing virtual global commons that affords small numbers of violent individuals the opportunity and capability to carry out a global insurgency and complex, devastating attacks. The expansion of the internet, linked to economic prosperity, is a two edged sword, improving people's standard of living while at the same time empowering those in violent disagreement with the values and concepts it embodies to attack its proponents more effectively.

RECOMMENDATIONS

The internet is here to stay as major component of the world's economic prowess and a highly visible presence in the process of globalization. The internet's rapid growth and penetration into all aspects of the industrialized and developing world has led it to become a part of a new "Virtual Global Commons." Since the internet is now an integral part of world civilization and has open access nature, there is no way to deny its use to the

insurgents/terrorists for their own criminal/violent agendas. Denying the internet as a distributed sanctuary is an impossibility for the US. Attempting to cut the insurgents/terrorists off from the internet and its massive networks, would display a complete lack of understanding of its capabilities and operation. A quote from an earlier era illuminates the challenge to the US in combating insurgents/terrorists on the internet.

> Little minds try to defend everything at once, but sensible people look at the main point only; they parry the worst blows and stand little hurt if they avoid a greater one. If you try to hold everything, you hold nothing.
>
> - Fredrick the Great[33]

There should be a two-pronged approach to addressing the insurgent/terrorist threat on the internet. The first approach is to manage the risk the internet possesses as an insurgent/terrorist command and control and intelligence collection tool. This is the classic concept of force protection and physical security. General information about a target is probably not deniable to the insurgents/terrorists. However, the US needs to deny the insurgents the detailed information about possible targets. This is a major component of the US Strategy for Defending Cyberspace.[34] The US is doing this and it will make the insurgent/terrorist's targeting process more difficult. In addition, the US needs to continue to harden it's own cyber-networks to minimize any direct collection and attack of vital network infrastructures through possible interfaces with the commercial/civilian internet. The insurgent/terrorist will likely use the internet as a means to launch cyberattacks against selected targets.

The second approach to addressing the hostile use of the internet is less traditional, as it seeks to exploit the insurgents/terrorists use of the internet rather than attempt to deny them access. The internet can work for the US as well as for the insurgents/terrorists. Insurgents/terrorists exploit the internet, but using the internet means that they have to utilize the technology it encompasses. The US needs to expand and enlarge the internet, adding more nodes and infrastructure. Not only will the US indirectly attack, using economic power, the source of peoples' frustrations and lack of hope that are a breeding ground for insurgent/terrorist beliefs and recruitment. The expansion of the internet will make it easier to track and monitor insurgent/terrorist organizations. The use of the internet leaves an electronic record, trail, or trace. Skilled operators and analysts can trace these links back to the insurgents/terrorists. The tracking information can then be turned over for more classic Human Intelligence or technical collection for targeting. The ability to operate dispersed also makes the insurgent/terrorist more vulnerable since they lack the personal situation awareness and protection that massing provides. The distributed, global nature of the internet allows the US to

conduct remote collection against insurgents/terrorists, minimizing the risk to US service members and increasing the efficiency of more traditional intelligence collection.

Additionally, the US needs to continue to encourage the expansion and use of the internet on a global basis in an effort to deny the insurgents/terrorists access to unaccountable operational funds. The free flow of undocumented currency allows the alliance or fusion of criminals and insurgents/terrorists to finance their operations and suborn people to provide them information and support. The increasing use of the internet as a mechanism for retail and business-to-business financial transactions not only avoids the inefficient use of hard currency, it also allows documentation of the financial trail. Tracing the financial transactions allows their exploitation by law enforcement agencies for arrest or the US for military targeting. The more financial transactions that travel across the internet the potential for less undocumented currency available to criminal or insurgents/terrorist organizations, limiting their ability to conduct and promote their operations.

The insurgents/terrorists use the internet as propaganda and a recruiting tool. Through websites and internet chat rooms, the insurgents/terrorists put out their message in an effort to influence and recruit. Again, the internet allows the US to monitor this process. The US could use information operations, promoting a dialog by using or hiring religious or political leaders to promote moderate viewpoints. Any communications created during this dialog would not only work to counter the insurgents/terrorist's message, but also creates yet another opportunity for active, targeted collection against the insurgents/terrorists.

Finally, the US, as it continues to promote globalization and seeks to transform many federal government organizations, needs to maintain a priority of monitoring and researching the internet. The relative "newness" of the internet and the distributed, nearly chaotic way in which it grows and operates, means that its capabilities and effects are poorly understood. Insurgents/terrorists are using the internet and constantly evolving their tactics and techniques. Although they have adapted their organizations to take advantage of the internet they have not yet evolved into "networked" insurgent organizations. The United States needs to remain vigilant as networked insurgent/terrorist organizations are still in their infancy. Through observation, research and simulation the United States, in cooperation with the private sector, needs to understand the capabilities and limitations the internet imposes on the insurgents/terrorists.

The internet offers both opportunities and challenges to the US as it creates and occupies a new global commons. The US will need to conduct a sustained strategic campaign to operate in this new environment and minimize its use as a distributed sanctuary and communications

tool for evolving insurgent/terrorist organizations. The US, in its pursuit of insurgents/terrorists, needs to make the internet a priority in its strategic endeavors. As General of the Army Douglas MacArthur, once suggested:

> We must hold our minds alert and receptive to the application of unglimpsed methods and weapons. The next war will be won in the future, not in the past. We must go on, or we will go under.
>
> - General of the Army Douglas MacArthur[35]

The opportunities and challenges the internet contains are great and Americans would ignore them at their peril.

WORD COUNT=4540

ENDNOTES

[1] The National Security Strategy of the United States of America dated September 2002 is the baseline federal document outlining the strategic security posture for the U.S. All other US Government and Department of Defense strategies flow from it.

[2] George W. Bush, National Security Strategy of the United States of America, Washington: The White House, September 2002, 17.

[3] David Held & Anthony McGrew, eds., The Global Transformation Reader, 2nd Edition. (Cambridge, UK: Polity Press, 2003), 3.

[4] Thomas L. Friedman, *The Lexus and the Olive Tree* (New York: Farrar, Straus, and Giroux, 1999), 93.

[5] Friedman, xv.

[6] Wayne Lee, To Rise from Earth (New York: Checkmark Books, 2000), 12. The height at which space begins is 121.9 Kilometers; at this altitude there is no atmospheric pressure on an object.

[7] Baylis, John. and others, Strategy in the Contemporary World (Oxford: Oxford University Press, 2002), 210.

[8] Joint Chefs of Staff, The US Department of Defense Dictionary of Military and Associated Terms (New York: Lionel Leventhal Limited, 1987), 317.

[9] Thomas X. Hammes, The Sling and the Stone (St Paul, MN: Zenith Press, 2004), 38.

[10] United States Congress, National Commission on Terrorist Attacks Upon the United States, The 9/11 Commission Report (New York: W.W. Norton and Company, 2004), 170.

[11] Rabasa, Angel M. and others, The Muslim World After 9/11 (San Monica, CA: RAND Corporation, 2004), 45.

[12] Brett F. Woods, The Art and Science of Money Laundering, (Bolder, CO: Paladin Press, 1998), 178-179.

[13] Hammes, 40.

[14] Rabasa, 44.

[15] Ibid, 40.

[16] J.F. Rischard, High Noon (New York: Basic Books, 2002), 29.

[17] Friedman, 325.

[18] Joint Chiefs of Staff, Joint Doctrine for Targeting (JP 3-60), VI. (accessed 9 February 2005); available from <http://www.dtic.mil/doctrine/jel/new_pubs/jp3_60.pdf>; Internet.

[19] Ibid, C-2.

[20] C.J.M. Drake, Terrorists' Target Selection (New York: St Martin's Press, 1998), 175-182.

[21] Norman Wade, The Operations Smartbook-FM 3.0 Operations (Florida: Lightening Press, 2002), 1-50 – 1-51.

[22] Rischard, 20.

[23] JP 3-60, C-3.

[24] Bruce Berkowitz, The New Face of War (New York: Free Press, 2003), 10.

[25] Ibid, 11.

[26] Walter Laqueur, Ed., Voices of Terror" Manifestos, Writings, and Manuals of Al Qaeda, Hamas, and other Terrorists from Around the World and Throughout the Ages (New York: Reed Press, 2004), 405-406. The stated second source of information for providing the other 20 percent of the needed information on a target is classic Human Intelligence (HUMINT) collection or espionage.

[27] Bruce Schneier, Beyond Fear: Thinking Sensibly about Security in an Uncertain World (New York: Copernicus Books, 2003), 88-89.

[28] George W. Bush, National Security Strategy of the United States of America, 1.

[29] Zalmay M. Khalilzad and John P. White, Eds., The Changing Role of Information in Warfare (Santa Monica, US: RAND, 1999), 253-281.

[30] JP 3-60, III-4.

[31] George W. Bush, National Security Strategy of the United States of America, 21.

[32] Friedman, 322.

[33] Peter G. Tsouras, ed., The Greenhill Dictionary of Military Quotations. (London: Greenhill Books, 2000), 137.

[34] George W. Bush, The National Strategy to Secure Cyberspace of the United States of America. (Washington: The White House, February 2008, xviii.

[35] Peter G. Tsouras, Warriors' Words: A Quotation Book. (London: Arms and Armour Press, 1992), 222.

BIBLIOGRAPHY

A.T. Kerney, Inc and the Carnegie Endowment for International Peace, *Globalization Index 2003.* New York: Carnegie Endowment for International Peace, 2003.

_____, *Globalization Index 2004.* New York: Carnegie Endowment for International Peace, 2004.

Barnett, Thomas P.M. The *Pentagon's New Map; War an Peace in the Twenty-First Century*. New York: G.P. Putnam's Sons, 2004.

Berkowitz, Bruce. *The New Face of War*. New York: The Free Press, 2003.

Brin, David. *The Transparent Society*. Massachusetts: Perseus Books, 1998.

Brockman, John, ed. The Next Fifty Tears; Science in the First Half of the Twenty-First Century. New York: Vintage Press, 2002.

Bush, George W., *National Security Strategy of the United States of America*, Washington: The White House, September 2002.

_____, *The National Strategy to Secure Cyberspace of the United States of America*, Washington: The White House, February 2008.

Baylis, John, ed. Strategy in the Contemporary World, Oxford: Oxford University Press, 2002.

Drake, C.J.M. *Terrorists' Target Selection*. New York: St. Martin's Press, 1998.

Friedman, Thomas L. *The Lexus and the Olive Tree*. New York: Farrar, Straus, and Giroux, 1999.

Halweil, Brian and Mastny, Lisa, Project Directors. *State of the World 2004*. New York: W.W. Norton & Company, 2004.

Held, David and McGrew, Anthony, Eds. *The Global Transformations Reader*. New York: Polity Press. 2003.

Hunter, Richard. *World Without Secrets*. New York: John Wiley & Sons Inc, 2002.

Johnson, Steven. *Emergence; The Connected Lives of Ants, Brains, Cities, and Software*. New York: Touchstone, 2001.

Joint Chiefs of Staff, *Dictionary of Military and Associated Terms* (JCS Pub 1). New York: Greenhill Books, 1987.

Joint Chiefs of Staff. *Joint Doctrine for Targeting (JP 3-60).* Washington, DC: GPO, 2002.

Khalilzad, Zalmay M. and White, John P., Eds. *The Changing Role of Information in Warfare*. Santa Monica: RAND, 1999.

Laqueur, Walter ed. *Voices of Terror*. New York: Reed Press, 2004.

Lee, Wayne. *To Rise from the Earth*. New York: Checkmark Books, 2000.

Mannes, Thomas X. *The Sling and the Stone*. St Paul, MN: Zenith Press, 2004.

Manwaring, Max G. Ed. The Search for Security; A U.S. Grand Strategy for the Twenty-First Century. Connecticut: Prager Publishers, 2003.

Moises, Naim. *Surprises of Globalization*. New York: Carnegie Endownment for International Peace, 2003.

Rabasa, Angel M. and others. *The Muslim World After 9/11*. Santa Monica, CA: Rand, 2004.

Renner, Michael Renner Project Director. *Vital Signs 2003*. New York: W.W. Norton & Company, 2003.

Rischard, J.F. *High Noon*. New York: Basic Books, 2002.

Sageman, Marc. *Understanding Terrorist Networks*. Pennsylvania: University of Pennsylvania Press, 2004.

Sakiko Fukuda-Parr Director. *Human Development Report 2004*. New York: United Nations Development Program, 2004.

Schneier, Bruce. Beyond Fear; Thinking Sensibly About Security in an Uncertain World. New York: Copernicus Books, 2003.

Smith, Dan. *The Penguin Atlas of War and Peace*. New York: Penguin Books, 2003.

_____. The Penguin State of the World Atlas, Seventh Edition. New York: Penguin Books, 2003.

Steele, Robert David. *On Intelligence; Spies and Secrecy in an Open World*. Virginia: OSS International Press, 2001.

Sterling, Bruce. *Tomorrow Now*. New York: Random House, 2002.

Tsouras, Peter G., ed., *The Greenhill Dictionary of Military Quotations*. London: Greenhill Books, 2000.

Tsouras, Peter G., *Warriors' Words: A Quotation Book*. London: Arms and Armour Press, 1992.

United States Congress National Commission on Terrorist Attacks Upon the United States, *The 9/11 Commission Report*. New York: W.W. Norton & Company, Inc., 2004.

Vicente, Kim. *The Human Factor*. New York: Routledge, 2004.

Wade, Norman M. *The Operations FM 3-0 Smartbook*. Florida: Lightening Press, 2002.

Woods, Brett F. *The Art and Science of Money Laundering*. Boulder, CO: Paladin Press, 1998.

Wright, Robert. *Nonzero; The Logic of Human Destiny*. New York: Vintage Books, 2000.